



Minnesota
Fusion Center

(U//FOUO) Minnesota Vikings 2018 Season

Risk Assessment



13.82

13.82

13.82

13.82

(U//FOUO) During the 2016 NFL Season, demonstrators gained unauthorized access to a restricted area at US Bank Stadium in order to hang a banner in support of the #NODAPL cause against pipeline construction in North Dakota. Currently, protests routinely occur in Minnesota against the replacement of the "Line 3" Enbridge pipeline through northern Minnesota. Given previous protests against pipeline activity, the MNFC assesses the likelihood of anti-pipeline demonstrations near or at US Bank Stadium is likely.

13.82

continued

(U) Conclusion

(U//FOUO) Due to the aforementioned key judgments, the Minnesota Fusion Center assesses the overall risk to these events as **MEDIUM**. The MNFC will continue to monitor open sources and provide pertinent information, should it become available after this assessment is issued.

(U//FOUO) If you have questions or concerns, please contact the **Minnesota Fusion Center** at **(651) 793-3730** or **mn.fc@state.mn.us**.

(U) 2018 MN Vikings Season Home Game Summary

Date	Time (Network)	Lineup
(Preseason) Saturday, 18 August	12:00pm (NFLN)	Jacksonville Jaguars at Minnesota Vikings
(Preseason) Friday, 24 August	7:00pm	Seattle Seahawks at Minnesota Vikings
Sunday, 09 September	12:00pm (FOX)	San Francisco 49ers at Minnesota Vikings
Sunday, 23 September	12:00pm (CBS)	Buffalo Bills at Minnesota Vikings
Sunday, 14 October	12:00pm (FOX)	Arizona Cardinals at Minnesota Vikings
Sunday, 28 October	7:20pm (NBC)	New Orleans Saints at Minnesota Vikings
Sunday, 04 November	12:00pm (FOX)	Detroit Lions at Minnesota Vikings
Sunday, 25 November	7:20pm (NBC)	Green Bay Packers at Minnesota Vikings
Sunday, 16 December	12:00pm (CBS)	Miami Dolphins at Minnesota Vikings
Sunday, 30 December	12:00pm (FOX)	Chicago Bears at Minnesota Vikings

SECURITY NOTE: The information contained in this document is classified For Official Use Only (FOUO). No portion of this document should be released to the media or general public. This document may contain data classified as confidential, nonpublic, and/or private data under Minnesota Government Data Practices Chapter 13 and subject to restriction. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924.

continued

(U) Appendix A: National Terrorism Advisory System Bulletin



National Terrorism Advisory System

Bulletin

www.dhs.gov/advisories

May 9, 2018 2:00PM EDT

SUMMARY OF TERRORISM THREAT TO THE U.S. HOMELAND

Since 2015, the Department of Homeland Security (DHS) has used this Bulletin to highlight the continuing terror threat to the U.S. Homeland. The United States is engaged in a generational fight against terrorists who seek to attack the American people, our country, and our way of life. An informed, vigilant and engaged public remains one of our greatest assets to identify potential terrorists and prevent attacks.

DURATION

This Bulletin will expire on **September 14, 2018** at 1:00 PM EDT

ADDITIONAL DETAILS

- We continue to face one of the most challenging threat environments since 9/11, as foreign terrorist organizations exploit the Internet to inspire, enable, or direct individuals already here in the homeland to commit terrorist acts. Homegrown terror suspects increasingly rely on technology, such as end-to-end encrypted social media applications, to avoid detection.
- Terrorist groups are urging recruits to adopt easy-to-use tools to target public places and events. Specific attack tactics have included the use of vehicle ramming, small arms, straight-edged blades or knives, homemade explosives, and poisons or toxins.
- Some terrorist groups overseas are using battlefield experiences to pursue new technologies and tactics, such as unmanned aerial systems and chemical agents that could be used outside the conflict zones. Additionally, terrorists continue to target commercial aviation and air cargo, including with concealed explosives.
- Violent extremist media encourages individuals worldwide to launch attacks using all means possible. Continued U.S. and partner successes in disrupting and defeating terrorists on the battlefield may encourage homegrown terrorists to carry out acts of violence in the homeland instead of attempting to travel overseas to fight or in retaliation for apparent losses.
- Additionally, foreign terrorist fighters who have acquired training and battle-tested terrorism experience may flee from terrorist-controlled territories with a desire to conduct attacks elsewhere, including the United States.

U.S. GOVERNMENT COUNTERTERRORISM EFFORTS

- DHS and the Federal Bureau of Investigation (FBI) continue to provide guidance to state, local, tribal and territorial partners related to the current threat environment. DHS also partners closely with the private sector to provide risk assessments and coordinate security measures with business owners and operators. The public may continue to observe law enforcement and security activity in and around public places and events.
- DHS protects the homeland from terrorism by working closely with the FBI and other intelligence partners to detect and disrupt terror suspects, putting in place additional screening and vetting measures to identify suspicious travelers and cargo, combating violent radicalization and terrorist recruitment in our communities, monitoring emerging threats, and engaging with foreign partners.
- More broadly, DHS remains committed to preventing violence and threats meant to intimidate or coerce specific populations on the basis of their religion, ethnicity or identity.

TYPES OF ADVISORIES

Bulletin

Describes current developments or general trends regarding threats of terrorism.

Elevated Alert

Warns of a credible terrorism threat against the United States.

Imminent Alert

Warns of a credible, specific and impending terrorism threat against the United States.

HOW YOU CAN HELP

- Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators.
- Report suspicious activity or information about a threat, including online activity, to fusion centers and the FBI's Field Offices – part of the Nationwide Suspicious Activity Reporting Initiative.
- Learn [how to recognize signs of pre-operational planning](#) associated with terrorism or other criminal activity.

BE PREPARED

- Be prepared for security and plan ahead. Anticipate delays and restrictions on items around populated places and at public events.
- Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs info with you.
- [Connect, Plan, Train, and Report](#) to prepare businesses & employees. Security tools/resources can be accessed through the DHS's [Hometown Security Campaign](#).

STAY INFORMED

- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.
- We urge Americans to continue to travel, attend public events, and freely associate with others but remain vigilant and aware of surroundings.
- The Department of State issues [international travel alerts and warnings](#).
- For additional information visit [Ready](#).

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides information on homeland security issues and threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates: www.twitter.com/dhsgov

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

continued

(U) Appendix B: SAR Card



Suspicious Activity Reporting Indicators and Behaviors

Tools for
Analysts and
Investigators

Behaviors	Descriptions
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents (classified or unclassified)), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.
Potential Criminal or Non-Criminal Activities Requiring Additional Information During Vetting	
<i>Note: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.</i>	
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

<http://nsi.ncirc.gov>

rev. 02/16

continued

(U) Appendix C: Private Security

Private Security

Private Security hired by the facility is a potential area of concern. In Minnesota, the Minnesota Board of Private Detectives and Protective Agents is responsible for approving licenses for private security firms and private detectives. The Board reviews all license applications upon initial request and every two years after initial approval. In the interim, it is incumbent upon the license holder to ensure that the firm is within legal requirements of Minnesota Statutes. It is rare that clients of the security firm conducts an audit, although it is advised. Should you have questions regarding private security, please contact the Minnesota Board of Private Detective and Protective Agents at (651) 793-2666. For your reference, pertinent Minnesota Statutes are summarized below (for complete Minnesota Statutes, visit <https://www.revisor.mn.gov/statutes/>).

Minnesota Statute 326.336 Employees of License Holders

Subdivision 1. Background Check

- The employee is a conditional employee until the employer receives a report from the bureau that the prospective employee has not been convicted in Minnesota of a felony or any offense listed;
- Background checks are conducted by both the MN BCA and the FBI.
- The employer shall immediately dismiss an employee who has been convicted of a disqualifying offense.

Subdivision 2. Identification Card

- An ID card must be issued by the license holder to each employee.
- The card must be in the possession of the employee at all times.
- The ID card must contain the license holder's name, logo (if any), address or Minnesota office address, and the employee's photo and physical description.
- The card must be signed by the employee and by the license holder, qualified representative, or Minnesota office manager.

Minnesota Statute 326.3361 Training

Subdivision 2. Required Contents

- 12 hours of pre-assignment or on-the-job certified training within the first 21 days of employment, or evidence that the employee successfully completed equivalent training, before the start of employment.
- Six hours a year of certified continuing training for all license holders, qualified representatives, Minnesota managers, partners, and employees.

Minnesota Statute 326.3381 Licenses

Subdivision 3. Disqualification

No person is qualified to hold a license who has:

Felony convictions	Acts in other countries that would be a felony in MN		
Criminal sexual conduct	Assault	Theft	Larceny
Burglary	Robbery	Unlawful entry	Extortion
Defamation	Buying/receiving stolen property		Escape
Possession/production/sale/distribution of narcotics unlawfully		Using/carrying burglary tools unlawfully	

continued

(U) Appendix C: Private Security (Continued)

Minnesota Statute 326.338 Persons Engaged as Private Detectives or Protective Agents

Subdivision 4. Protective Agent

- A person who for a fee, reward, or other valuable consideration undertakes any of the following acts is considered to be engaged in the business of protective agent:
- providing guards, private patrol, or other security personnel to protect persons or their property or to prevent the theft, unlawful taking of goods, merchandise, or money, or to prevent the misappropriation or concealment of goods, merchandise, money, or other valuable things, or to procure the return of those things;
- physically responding to any alarm signal device, burglar alarm, television camera, still camera, or a mechanical or electronic device installed or used to prevent or detect burglary, theft, shoplifting, pilferage, losses, or other security measures;
- providing armored car services for the protection of persons or property;
- controlling motor traffic on public streets, roads, and highways for the purpose of escorting a funeral procession and oversized loads; or
- providing management and control of crowds for the purpose of safety and protection.

A person covered by this subdivision may perform the traffic-control duties in clause (4) in place of a police officer when a special permit is required, provided that the protective agent is first-aid qualified.